ly

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/402,144	09/29/1999	MARTINA HANCK	P991784	5593

29177 7590 02/03/2005

BELL, BOYD & LLOYD, LLC
P. O. BOX 1135
CHICAGO, IL 60690-1135

EXAMINER	
KIM, JUNG W	
ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 02/03/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/402,144	HANCK ET AL.	
	Examiner	Art Unit	
	Jung W Kim	2132	

-- The MAILING DATE of this communication appears on the cov r sh et with the correspond nce address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 13 July 2004.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-3,10-12 and 19-48 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) 1-3,10-12 and 19-48 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-3, 10-12 and 19-48 have been examined. A Response to the Office Action was filed on July 13, 2004; no amendment to the claims was filed in the response.

Response to Arguments

2. The following is a response to the arguments presented on pages 2-3 of the "Response to the Office Action" filed on July 13, 2004.

3. Applicant's arguments, see page 2, 2nd paragraph, with respect to the 35 U.S.C. 112, first paragraph rejections of claims 28, 29 and 43-45 have been fully considered and are persuasive. The 112, first paragraph rejections of claims 28, 29 and 43-45 has been withdrawn.

4. In regards to Applicant's argument that "one of ordinary skill in the art would find no motivation, either in the teachings of Halsall or in the knowledge known in the art, to utilize a method for encoding text with a commutative checksum, when the commutative checksum already achieves this objective" (see Remarks, page 3, 2nd paragraph, 3rd sentence), examiner disagrees. Checksums are error detection functions that are implemented to identify errors in the transmission of data; these functions are well known to one of ordinary skill in the art as identified by the prior art of record, and

further, a checksum value (or a commutative checksum value) would trivially be susceptible to modification and/or evaluating by an unscrupulous party since checksum algorithms are publicly known. Encryption functions are cryptographic means to prevent a third party from uncovering and/or modifying data hidden by the encryption function. These functions are distinct from other coding functions because, inter alia, they incorporate a secret key (symmetric or asymmetric) within the function to prevent a determined party from exploiting secured data. Cryptographic functions are designed so that even if the implementation of the function is known by an attacker (most crypto functions are published), a brute force attack to uncover the secret key, and hence the encrypted data, is infeasible. For example, RSA and triple DES are standard crypto functions wherein the implementation is publicly known and where the security of the function is reliant on a secret key. In summary, as taught by Halsall, cryptographic functions are implemented to secure data within a message transmission and checksum values are data values inserted into the transmission to indicate the original integrity of the message as submitted by the sender. See Halsall, pages 128-129 and page 719, 2nd paragraph.

5. To further substantiate the use of a cryptographic operation to protect an integrity value, the independent claims are rejected under Halsall in view of Frezza.

Claim Rejections - 35 USC § 103

6. Claims 1-3, 10-12, 19-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Halsall, <u>Data Communications, Computer Networks and Open</u>

Systems 4th Edition (hereinafter Halsall) in view of Frezza et al. U.S. Patent No. 4,982,430 (hereinafter Frezza).

7. As per claim 10, Halsall teaches a block sum check, also known as a two-dimensional parity check, which forms a commutative checksum on digital data. This block sum check is arranged as follows:

a. digital data is grouped into several data segments by a computer and processed to form a first segment checksum for each data segment. The first segment checksum constitutes the assignment of an odd or even parity bit to each block. This assignment is given the operational name of row parity (see Halsall, page 129, 1st paragraph);

b. the first segment checksums are processed to form a first commutative checksum (Halsall, page 129, 1st paragraph). The first commutative checksum constitutes an assignment of a parity bit (odd or even) for each bit position for all the blocks of a message, including the parity bit position of each block. This assignment is given the operational name of column parity and the block comprising the column parity bits is the first commutative checksum. In addition, Halsall teaches using an XOR operation to establish parity, which is a commutative operation (see Halsall, page 128, Figure 3.14);

c. the arrangement is incorporated into the sending side of a pair of Data Terminal Equipment (DTE) (see Halsall, page 125, section 3.4 and page 128, section 3.4.2). Conventionally, DTE incorporates at least one arithmetic/logic

unit: ALUs are the basic units required in hardware to perform arithmetic and logic microoperations.

8. Although Halsall does not cover a cryptographic operation to protect the first commutative checksum in this section (the section covers error detection methods), Halsall in a different section teaches data encryption operations as standard implementations on transmissions that require privacy on an unprotected network (see Halsall, page 719, 2nd paragraph). Furthermore, error correction protocols and data encryption protocols are distinctly layered and hence require no additional modification to their respective protocols to be implemented together on a network. However, Halsall does not expressly teach cryptographically protecting integrity values of a message. Frezza teaches encrypting integrity values to prevent unauthorized alteration of a message. See Frezza, col. 2:45-3:13. It would be obvious to one of ordinary skill in the art at the time the invention was made to implement a cryptographic operation to secure the first commutative checksum. Motivation to combine prevents an unscrupulous third party from an unauthorized modification of a transmitted message. See Frezza, col. 2:20-25. The aforementioned cover claim 10.

9. As per claim 11, Halsall in view of Frezza cover an arrangement as outlined above in the claim 10 rejection under 35 U.S.C. 103(a). In addition, the arrangement also includes the following:

a. the allocation of the predetermined cryptographic checksum to the digital data and the subjection of the cryptographic commutative checksum to an

inverse cryptographic operation to form a first commutative checksum (see Halsall, page 723, 1st paragraph). Halsall teaches any message encrypted by DES has an inverse operation (decryption) to retrieve the original message (see Halsall, page 723, 1st paragraph). Furthermore, every ciphertext is associated with a specific plaintext;

b. the formation of a second segment checksum for each data segment, the formation of a second commutative checksum by a commutative operation on the second segment checksums, and a comparison of the first commutative checksum and the second commutative checksum for a match (see Halsall, page 129, Figure 3.15 (b)).

The aforementioned covers claim 11.

10. The above arrangements outlined in the claim 10 and 11 rejections under 35 U.S.C. 103(a) together covers the arrangement outlined in claim 12.

11. As per claims 37-39, Halsall in view of Frezza cover the following: 1) an arrangement for forming a first commutative checksum, 2) an arrangement for checking a predetermined cryptographic commutative checksum, and 3) an arrangement for forming and checking a first commutative checksum as outlined above in the claim 10, 11, and 12 rejections under 35 U.S.C. 103(a). In addition, the cryptographic operations described use a symmetric key methodology (see Halsall, page 723, 1st paragraph).

12. As per claims 40-42, Halsall in view of Frezza cover the following: 1) an arrangement for forming a first commutative checksum, 2) an arrangement for checking a predetermined cryptographic commutative checksum, and 3) an arrangement for forming and checking a first commutative checksum as outlined above in the claim 10, 11, and 12 rejections under 35 U.S.C. 103(a). In addition, Halsall teaches the commutative operation to establish column parity, which forms the commutative checksums, is an XOR operation (see Halsall, page 127, section 3.4.1): the XOR operation exhibits both commutative and associative properties. Furthermore, control of the data inputs to the arithmetic circuits of the ALU determines the type of operation executed by the ALU. The aforementioned cover claims 40-42.

13. As per claims 43-45, Halsall in view of Frezza cover an arrangement as outlined above in the claim 11-12 rejections under 35 U.S.C. 103(a). Halsall does not expressly disclose archiving the digital data and the cryptographic commutative checksum. However, archiving the elements of a transmission are standard features to verify the contents of a transmission to an auditor. The examiner takes Official Notice that archiving transmission elements are standard means to record the transmission to prove the contents and status of the transmission at a latter date (i.e. auditing a transmission). It would be obvious to one of ordinary skill in the art at the time the invention was made to archive the digital data and the checksum. Motivation to combine preserves a receipt of the transmission.

14. As per claims 46-48, Halsall in view of Frezza cover the following: 1) an arrangement for forming a first commutative checksum, 2) an arrangement for checking a predetermined cryptographic commutative checksum, and 3) an arrangement for forming and checking a first commutative checksum as outlined above in the claim 10, 11, and 12 rejections under 35 U.S.C. 103(a). In addition, as mentioned previously, the digital data is cryptographically protected, and by convention, the cryptographic operation would be implemented by an ALU. Furthermore, since Halsall teaches the arrangements in the context of a digital network, the digital data would necessarily be processed in accordance with a network management protocol. The aforementioned cover claims 46-48.

15. As per claims 1-3 and 22-33, they are method claims corresponding to claims 10-12, 37-48 and they do not teach or define above the information claimed in claims 10-12, 37-48. Therefore, claims 1-3 and 22-33 are rejected under Halsall in view of Frezza for the same reasons set forth in the rejections of claims 10-12, 37-48.

16. As per claims 34-36, Halsall in view of Frezza cover the following: 1) an arrangement for forming a first commutative checksum, 2) an arrangement for checking a predetermined cryptographic commutative checksum, and 3) an arrangement for forming and checking a first commutative checksum as outlined above in the claim 10, 11, and 12 rejections under 35 U.S.C. 103(a). However, the parity check described in the aforementioned methods for forming the segment checksums are not in accordance

with a type from the group consisting of a hashing value, a CRC code, and a cryptographic one-way function as specified in the applicant's claims. In a separate section, Halsall does teach that a CRC code is used in lieu of the parity check for more reliable detection of transmission errors such as burst errors (see Halsall, page 130, section 3.4.3). It would be obvious to one of ordinary skill in the art at the time the invention was made to form the segment checksums using CRC instead of parity checking. The motivation for using CRC enables a more reliable detection of transmission errors for each segment as taught in the separate section of Halsall.

17. As per claims 19-21, they are method claims corresponding to claims 34-36 and they do not teach or define above the information claimed in claims 34-36. Therefore, claims 19-21 are rejected under Halsall in view of Frezza for the same reasons set forth in the rejections of claims 34-36.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (571) 272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

Jk
January 31, 2005

Gilberto Barron

GILBERTO BARRON Jr.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100